MANAGING PERSONAL INFORMATION POLICY

Author - M Vevers

Last reviewed - July 2015

Next review date - July 2018

Reviewed by - Laurus Trust

Statutory basis for the policy:

Data Protection Act 1998
Freedom of information Act 2000

Reviewed by:	Records & Information Governance Group (RIG) Information Management Steering Group (IMSG) Information Management Strategy Group Adults Social Care Information Governance Freedom of Information/Data Protection Officer Corporate Records Manager ICT – Managing for Change Project Manager

Managing Personal Information Policy

1. Introduction

1.1. The The Laurus Trust recognises the need to protect personal data and places great emphasis on ensuring it remains secure and confidential. This policy applies to our manual and electronic records as well as to conversations we have about service-users and the services they receive.

1.2. Everyone working for the Trust must be aware of the requirements of the Data Protection Act 1998 (DPA) and their duty to keep personal data secure and confidential. This includes ensuring we only share personal data where we have the legal power to do so. This policy applies to all employees of the Trust including temporary, agency and contract staff.

2. Definitions

2.1. 'Personal data' (often referred to as personal information) are data which relate to a living identifiable individual.

'Data subject' is an individual who is the subject of the personal data.

'Data controller' is an individual or organisation which processes personal data, such as CHHS or one of its partners.

'Processing' means any action performed on the data, including collecting, amending or simply holding them.

2.2. This policy applies to any and all personal data processed by or on behalf of CHHS. Data subjects can be any individuals but the service providers are most likely to be students and their families and employees of the Trust.

3. Data protection principles

3.1. The Laurus Trust recognises the importance of data protection and complies with all the provisions of the DPA when processing personal data. The DPA contains eight data protection principles of good information handling which employees must ensure they comply with at all times. These principles are outlined below:

1. Personal data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and where necessary, kept up-to-date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights given to data subjects by the DPA.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4. Data Principles – The Laurus Trust employees are to follow the Caldicott principles detailed below:-

Principle 1 **Justify the purpose.**
Every proposed use or transfer of person-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2 **Do not use person-identifiable information unless it is absolutely necessary.**
Person-identifiable information should not be used unless there is no alternative.

Principle 3 **Use the minimum necessary person-identifiable information.**
Where use of person-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identification.

Principle 4 **Access to person-identifiable information should be on a strict need-to-know basis.**

Only those individuals who need access to person-identifiable information should have access to it and they should only have access to the information they need to see.

Principle 5 **Everyone should be aware of their responsibilities.**
Action should be taken to ensure that those handling person-identifiable information are aware of their responsibilities and obligations to respect individual confidentiality.

Principle 6 **Understand and comply with the law.**
Every use of person-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

5. Personal information

5.1. The Laurus Trust will ensure that the personal data it records and otherwise processes are adequate and relevant to the purpose or purposes for which they are required.

5.2. The Laurus Trust's records may contain the following types of personal information:

Identification details: Names, addresses, National Insurance numbers, disabled person's numbers.

Personal characteristics: Age, sex, date of birth, physical description, habits, facts about the person.

Family circumstances: Marital details, family details, household members, social contacts.

Social circumstances: Accommodation details, leisure activities, lifestyle.

Financial details: Income, expenditure, bank details, allowances, benefits and pensions.

Other information: Employment details; qualifications, skills and professional expertise; services requested/required and currently obtained; referrals/assessments; details of complaints, accidents or incidents; court, tribunal or enquiry details, CCTV images.

This is not an exhaustive list and should not be taken as such.

6. Sensitive personal information

6.1. The DPA makes a distinction between personal data and sensitive personal data. Personal information which individuals may perceive as being of a sensitive nature is not necessarily 'sensitive personal data' in data protection terms. In the DPA, sensitive personal data means personal data consisting of information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- commission or alleged commission of any offence; or in relation to
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

6.2. Extra care must be taken when processing sensitive personal data. Before recording or otherwise processing sensitive personal information, the Laurus Trust must be satisfied that it can meet one or more of the conditions specified in the DPA which allow the processing to take place. Generally we can and will process sensitive personal data if it is necessary in order to provide services which we are required to provide by statute, the individual has given his or her explicit consent or it is required for legal proceedings. There are other situations in which we can process this type of information and if employees are uncertain, they must seek advice.

7. Collection of personal information

7.1. Personal information may be collected for the following purposes:

- Ensuring students and their families are provided with the best service available.
- Maintaining a record of information about service-users to identify and provide the services which are appropriate to their needs.
- Providing information for the management of resources.
- Assisting in the forward planning, monitoring and evaluation of services.
- Maintaining records of resources to assist in the provision of services.
- Maintaining a record of the statutory duties and other legal requirements carried out.
- Maintaining a record of service-users' contacts with departments.
- Acting as agents to assist others in providing a service.
- Performing administrative and financial functions relating to service provision.

- Assessing the eligibility of service-users for benefits and services.
- Providing statistical returns and maintaining statutory registers.
- Assisting with research and training.
- Identifying needs and resources in the community.
- Assisting with supervision and work management.

7.2. Before collecting personal data, staff must offer proof of identity and wherever possible, they must explain to staff and/or students, or their recognised representative, why the information is required and what it will be used for. This may be done via the students' journals/Sims data sheets/VLE or for employees information is available on the The Laurus Trust website

8. Management of personal information

8.1. The Laurus Trust is committed to ensuring that all staff comply with the DPA and related legislation when they process personal data. Day-to-day management of personal information may include creating, sharing, destroying, storing, exchanging or verbally communicating information including visual images both electronically and manually (e.g. paper files or microfiche etc.). All staff must ensure they consider the following when they process personal information:

Relevance: Personal information obtained, used and shared must be relevant to providing services to the school community.

Accuracy: The Laurus Trust will supply and/or publish accurate information and keep personal information up-to-date.

Openness: The Laurus Trust is committed to being open about the way it uses, manages and otherwise processes personal information. If we share personal data we will always ensure it is done securely and in accordance with legislative requirements. We will obtain data subjects' written consent before sharing personal data with partner organisations unless there is no requirement to do this.

If an individual states they do not want their personal data to be provided to a specific partner organisation, his or her wishes will be followed if possible. There are circumstances where this is not possible, for example if we are required to do so by statute or court order or to prevent or detect a crime. Personal data shared under any such circumstances will be done so in line with our current information sharing protocols.

Personal information will only be published in an anonymous or aggregated form.

Security: Appropriate measures will be taken in accordance with legislative requirements to ensure personal data are kept secure and are not disclosed to unauthorised third parties.

Staff training: The Laurus Trust is committed to training all staff who access or otherwise process personal information in accordance with this policy.

Accessibility: The Laurus Trust will have clear, transparent policies and procedures in place to enable individuals such as employees, service-users and any other data subjects to access the personal data the Trust processes about them. This is one of the rights given to data subjects by the DPA. Data will be retained for as long as necessary in both Legal and Operational terms as required.

9. Users of personal information

9.1. There are two categories of people who may use the information held by the Trust:

- Authorised employees who require the information for authorised purposes.
- Other people or organisations that meet the Trust's disclosure criteria and have their own data protection policies in place which ensure at least the same level of protection as the Trust.

10. Information sharing

10.1. The Laurus Trust will share personal data with its specified partners in accordance with data sharing protocols which observe legislative guidelines on information sharing. The DPA guidelines govern how we can share personal information with our partner organisations and we must always comply with these frameworks. The general rules can be summarised as:

- Justify the purpose of using confidential information.
- Only identify the client/service user if necessary.
- Use the minimum amount of information required.
- Access should be on a strictly need-to-know basis.
- Everyone should be aware of their responsibilities.
- Everyone should understand and comply with the law.

11. Disclosure criteria

11.1. Some of the circumstances in which personal information may be disclosed are:

- where permission of the service-user has been given and the disclosure is permitted by law;
- where we have a statutory duty to disclose or by order of a court;
- for study, research or statistical purposes where the information has been anonymised;
- to prevent harm to the data subject or another person;
- where there is a risk to public health; or
- to prevent or detect a crime.

12. Archiving and destruction of personal information

12.1. When a file is closed it will be retained within the academy's archive system for a pre-defined period appropriate for that type of record. Personal information will be destroyed in an appropriate and secure manner. It will not be destroyed prematurely (in both legal and operational terms); nor will it be retained for longer than is necessary. Further information relating to retention schedules and destruction processes can be obtained from the Deputy Headteacher acting as Information Governance (IG) Lead at CHHS by contacting 0161 485 7201.

13. Security measures for personal information

13.1. The Laurus Trust is committed to ensuring personal data are secure at all times. Employees will act in accordance with accepted procedures and the guidelines outlined in the appendices to this policy and the Trust's Acceptable Use Policy for ICT.

13.2. Any incident which puts the security of personal information at risk must be reported in line with the Serious Information Governance Incident Procedure. Incidents involving the loss or compromise of IT equipment and personal data should also be reported to The Headteacher of the appropriate academy within the Trust and the IG Lead of the Trust.

14. Working away from academy premises

14.1. The Laurus Trust recognises that some employees will need to operate away from academy premises as part of their daily duties.

14.2. Any member of staff working away from academy premises will ensure that their working practices comply with the Data Protection Act 1998 and have due regard for the security and proper management of personal information, as well as their personal safety. All such employees will comply with the guidance in the Trust's Staff Acceptable Use Policy for ICT.

15. Service-user access to personal information

15.1. The DPA gives individuals the right to access all the personal data a data controller processes about them through the right to access records under the Education Act. This is the right of subject access and the Trust will assist individuals wishing to make a subject access request. Individuals are entitled to be provided with any information which constitutes their personal data unless the information is exempt. These requests must be dealt with in line with the provisions of the DPA and the Trust's policy and employees should seek advice where necessary.

15.2. Any employee who receives a subject access request directly from another individual must forward it to the IG Lead. The contact details are:

The Information Governance Lead
The The Laurus Trust
Woods Lane
Cheadle Hulme
Cheshire
SK7 7JY

Or enquiries@laurusTrust.sch.uk

16. Complaints

16.1. If an individual wishes to complain about the personal data we process about them they should be supported in this decision. Staff should provide advice and inform them of the academy complaints procedure. Advice should be sought from the IG Lead/HR Lead if required.

17. Breach of the policy

17.1. This policy is based on the legal requirements of the DPA; therefore breach of the policy may be a breach of the law. Most contraventions of the DPA are civil offences; however some are criminal offences. Negligent, reckless or deliberate breaches of the DPA which are likely to cause substantial damage or substantial distress may lead to CHHS being issued with a monetary penalty of up to £500,000 by the Information Commissioner's Office. With this in mind, breaches of the policy will be treated seriously by the The Laurus Trust and will be subject to a full investigation, in line with the Trust's disciplinary processes.

18. References

- Data Protection Act 1998
- Staff Acceptable Use Policy of ICT
- SIGI
- Disciplinary Policy

19. Consultation

- The The Laurus Trust IG Team
- The The Laurus Trust Governing Body
- Stockport IG Lead

Appendix A

Guidance for staff in handling and storing information

- Papers, files, audiovisual recordings, computer disks, microfiche or other media that contain personal data must be kept in locked cabinets, cupboards, drawers etc. when the offices are vacated and not placed in trays, pigeon holes etc.

- The keys to cabinets, cupboards, drawers etc. should be kept in a central locked key cupboard which has designated key-holders. Spare keys should be kept so that documents can still be accessed should a member of staff be away from work. Keys should not be left out if staff are away from their desks even for a short period of time.

- Any staff member with access to documents in any format which contain personal data will be responsible for ensuring they only seek information which relates to their duties and not for curiosity or other non-professional reasons.

- Where possible, non-electronic documents should be kept in parts of the building protected by an alarm system.

- Staff should ensure that personal information is not provided to any unauthorised person.

- Non-electronic documents containing personal information must be posted in sealed envelopes which are properly addressed, clearly marked e.g. ‘private and confidential’ and sent via recorded delivery where possible.

- Staff must ensure that documents containing personal data are returned to appropriate filing systems as soon as possible so they are easy for other employees to locate and always available for use.

- Documents (or any other items e.g. CDs, DVDs or USB sticks) containing personal data should not normally be taken off CHHS premises. Where this is unavoidable the items must be rigorously safeguarded at all times. All electronic information must be encrypted. Items must not be left in cars. A record must be made of who has the items, particularly if they are the only copies, in case urgent access to the information is required. Outside office hours the employee will be responsible for the security of the items in line with the guidance in paragraph 14.2

- All non-electronic material which contains personal data and has been authorised for disposal must be shredded or incinerated. Electronic documents (including back-ups) must be completely erased on a regular basis and not kept for longer than is necessary in accordance with the relevant retention schedule.

- In Reception, other public areas and around the working environment employees must ensure that documents, including those on computer screens, are not visible to non-Trust employees or employees who do not have the right to view the information.

- All staff have a responsibility to ensure that their desk area is kept tidy and

available for the next person to work – this means no personal possessions or paperwork should be left out or in trays etc. at any time.

Telephone enquiries

- Personal data or other confidential information must not be provided to telephone callers unless the staff member has satisfied themselves as to the identity of the caller and is certain that it is necessary to provide the information.

- If a staff member cannot confirm the caller's identity or has reason to doubt the identification provided they must make additional checks and telephone the caller back, using a telephone number from our existing records rather than one provided by the caller.

- If an employee has any doubts about whether to disclose personal data they should ask the caller to submit a written request for the information and seek guidance from their line manager or another appropriate senior manager.

Fax machines

All employees are required to read and understand the guidance on sending personal and sensitive e-mails and faxes outside of the organisation and review your own existing arrangements to see how they can be improved:

- The location of fax machines is important. They should not be placed in view of unauthorised personnel or visitors.

- Faxing should not be treated as a secure method of communication.

- Confidential personal information should not normally be sent by fax unless the recipient can assure you that the document will be removed from the fax machine by an authorised person upon receipt.

- Fax message header sheets must include a standard 'Privacy and Confidentiality Notice' in accordance with service guidelines.

- All fax front sheets should include the following statement:

  'Confidentiality Notice: The information contained in this fax is for the intended recipient(s) alone. It may contain personal information and/or data which is confidential information that is exempt from disclosure under English law and if you are not the intended recipient, you must not copy, distribute or take any action in reliance on it.

  If you have received this fax in error, please notify us immediately either by telephoning the sender of by contacting us at the address on the fax.'

Electronic records (including e-mails) – see above link

- Personal information held electronically is no different to personal information held in any other format so must comply with the DPA and this policy as well as the Trust's Staff Acceptable Use Policy for ICT and directorate-specific retention guidelines.

- Electronic documents containing personal information should whenever possible be stored in an appropriately secure network location.

- Personal information should not be stored off the network without explicit permission from the Trust ICT Manager. Where permission has been granted personal information should only be stored on equipment owned or leased by the Trust. Such storage will include the use of appropriate security measures. No personal information should be stored on any removable media e.g. USB sticks, CDs unless they are encrypted.

- Transmission of electronic documents containing personal information will always use the appropriate security protocols:

  Risks

  Emails are not a secure method of communication. They can go astray, be intercepted or be forwarded on to a number of people who are not entitled to see them within minutes. They can also be addressed incorrectly - people could type in an address incorrectly or select a name from the suggestions which appear when typing into the 'To' field and accidentally send the email to the wrong recipient. This also applies to emails meant for internal recipients; they can easily be sent to the wrong recipient or even an external recipient by mistake. If the email is not encrypted, the personal information in it will be disclosed to people who are not entitled to see it.

  Guidelines

  The simplest way to protect an e-mail sent internally or externally is to password protect and encrypt the attached file. If is just an e-mail message, write what you want to say in a Word document, save it as a password-protected file and select advanced options to encrypt it, attach the file to an email then send the email.

  If you are using MS Office 2010, you can encrypt the document by clicking on the 'file' tab, then clicking on 'protect document' under the 'Permissions' section, then choosing 'Encrypt with password' and follow the instructions on screen.

  As with fax front sheets a similar message needs to be included within your address cards/signatures on all emails which are also being sent out, with immediate effect please include the following at the end of your address card within email:

  Confidentiality*: This email, its contents and any attachments are intended only for the above named. As the email may contain confidential or legally privileged information, if you are not, or suspect that you are not, the above named or the person responsible for delivery of the message to the above named, please*

delete or destroy the email and any attachments immediately and inform the sender."

- Check, check and check again that you are sending your email to the intended recipient
- Remember that emails are the same as any other type of document or official communication.
- Do not retain them if there is no business or legislative need for the information they contain.
- Remember that anything you write in an email could be disclosed to the public under FOI or EIRs or disclosed to an individual if it is about that person.
- Anything you write in an email could be forwarded on to anyone once you have sent it; remember they are not secure or private! Ensure you password protect and encrypt any documents being sent via an email if containing personal information.

- Computer systems must be password-protected. Passwords must not be written down or disclosed and employees must not allow colleagues to use their individual usernames and passwords.

- When leaving desks for any period of time or to attend a meeting, staff should lock their computer using the Control + Alt + Delete function. Computer monitors must not be positioned where they can be seen by unauthorised people.

- Printouts must be kept under the same secure conditions as other non-electronic documents containing personal information – separate from pen drives where possible as paper cannot be encrypted.

- All staff must log out of their computer fully and ensure the monitor is switched off before leaving the office to go home. Laptops must be removed from desks and locked away in a secure place.

Audiovisual records

- Photographs of individuals should not be used unless you have obtained consent from them via the data collection sheet. In addition, individuals must be informed of the intention to publish at the time the photo is taken and must not object. If a photograph is to be used for a purpose other than those listed on the data collection sheet, permission should be sought from parents/carers

- Particular care must be taken when re-using photographs of individuals. Consideration must be given to the possibility that with the passage of time, death, illness or family tragedy has occurred meaning the re-use of a photograph may cause distress. Where there is any doubt regarding an individual, the photograph should not be used and a new photograph of another individual should be commissioned.

Appendix B

Home-working and mobile-working

When working from home, compliance with the Data Protection Act 1998 is just as important as it is when you are working at the Trust. This guidance will outline some of the things you must consider when working from home.

The guidance should be read in conjunction with the rest of the Managing Personal Information Policy.

- When working away from the Trust's premises, you should only ever use authorised and controlled access to IT equipment e.g. laptops, 'smart phones', removable media which are encrypted, password-protected or are otherwise secure. No other IT equipment should be used to store academy information, including personal information in any place other than the academy network.

- Take care when travelling to and from the Trust's premises or making journeys with IT equipment or paper copies of personal information. Consider your personal safety. Wherever possible, paper documents containing personal information and laptops or other IT equipment should not be left in cars for any length of time; they should be taken with you to meetings and visits and into your home at the end of the day.

- When working at home or at another location away from the Trust, be aware of your environment and the need to keep personal information secure. Security and privacy implications are the same as when you are working in the office; family members, friends, workmen or any other third parties who may be in your home while you are working must not have access to any personal information you are working with. This includes paper documents as well as access to your emails, the academy network and telephone discussions. Encryption passwords and your personal password to log on to the academy network must not be written down, even at home and must not be shared with any other individuals.

- Any papers e.g. notes, memos, lists, diaries, files or other documents containing personal information must not be left anywhere where they are visible to third parties. This includes leaving them on car seats or about your home.

- If you are working with paper files or have a printer at home, please ensure that nothing containing personal information is discarded with your normal household waste. Any documents containing personal information should be brought back to the Trust and securely destroyed using the confidential waste bins.

- When working with paper files containing personal information at home, you must minimise the amount of personal information contained in the documents or forms in case the paperwork is lost or stolen. This means that if the paperwork falls into the hands of a third party, individuals are much less likely to be identified and their privacy is protected.

- When taking the only copies of paperwork or files to work on while you are away from the Trust, you must sign out the files so that anyone wishing to access them knows when they were removed and also record within your case management system (if you use one) who has them and where they are. Any files and paperwork must remain secure and be returned to the Trust and signed in as soon as possible.

Appendix C

Security Risk Incident Form

Service Area	
Office location	
Manager Contact	
Office Manager	
Date of incident	
Type of data *	

Details of incident
Corrective action taken

Signed…….. Date……

Designation……